The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
10/17/2019

SUBJECT:
A Vulnerability in Juniper Junos OS Could Allow for Denial of Service

OVERVIEW:
A vulnerability has been discovered in Juniper Junos OS, which could allow for denial of service. Junos OS is a FreeBSD-based operating system used in Juniper Networks routers. This vulnerability specifically affects MX Series routers configured with SIP ALG and NAT. An attacker can exploit this issue by sending specially-crafted SIP packets. Repeated successful exploitation of this vulnerability could result in prolonged denial of service conditions.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED
This issue affects Juniper Networks Junos OS on MX Series:

- 16.1 versions prior to 16.1R7-S5;
- 16.2 versions prior to 16.2R2-S11;
- 17.1 versions prior to 17.1R3;
- 17.2 versions prior to 17.2R3-S3;
- 17.3 versions prior to 17.3R3-S6 ;
- 17.4 versions prior to 17.4R2-S8, 17.4R3;
- 18.1 versions prior to 18.1R3-S3;
- 18.2 versions prior to 18.2R3;
- 18.3 versions prior to 18.3R2;
- 18.4 versions prior to 18.4R2.

RISK:
Government:

- Large and medium government entities: **HIGH**
- Small government entities: **HIGH**

Businesses:

- Large and medium business entities: **HIGH**
- Small business entities: **HIGH**

Home Users: **LOW**

TECHNICAL SUMMARY:

A vulnerability has been discovered in Juniper Junos OS, which could allow for denial of service. The vulnerability specifically affects MX Series routers configured with SIP ALG and NAT. The Session Initiation Protocol (SIP) is a signaling protocol for initiating, modifying, and terminating multimedia sessions over the internet. An attacker can exploit this issue by sending specially-crafted SIP packets to crash the MS-PIC component on MS-MIC or MS-MPC. Repeated successful exploitation of this vulnerability could result in prolonged denial of service conditions.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Juniper to vulnerable systems immediately after appropriate testing.
- Disable SIP ALG on affected systems if not required by your organization.
- Restrict access to devices and applications from only authorized users and hosts.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Juniper:
https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10964&cat=SIRT_1&actp=LIST

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0065

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov

iTS Mississippi Department of
Information Technology Services
3771 Eastwood Drive | Jackson, Mississippi 39211-6381

DISCLAIMER: This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited